

## MATH237 — Discrete Mathematics

# Division & Factorization

### M-Strand, Lecture 2

## Division of Integers

In this section we work with the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

With addition and subtraction, for any  $a, b \in \mathbb{Z}$  it is true that the numbers  $-a$ ,  $-b$ ,  $a + b$  and  $a - b$  all remain in  $\mathbb{Z}$ .

For multiplication,  $ab \in \mathbb{Z}$ , but  $\frac{1}{a}$  and  $\frac{1}{b}$  are not elements of  $\mathbb{Z}$ .

Nevertheless, some quotients  $\frac{a}{b}$  do give numbers in  $\mathbb{Z}$ .

We want to study this more closely.

**Definition.** Suppose that  $a, b \in \mathbb{Z}$  and  $a \neq 0$ . Then we say that  $a$  **divides**  $b$ , denoted  $a \mid b$ , if there exists  $c \in \mathbb{Z}$  such that  $b = ac$ .

We also say that  $a$  is a **divisor** of  $b$ , or that  $b$  is a **multiple** of  $a$ .

2

## Division of Integers

Here are some simple examples and properties of ‘divides’ as defined in this way.

**Examples:** We have  $2 \mid 6$ , and  $13 \mid 78$ , and  $25 \mid 125$ , and  $7 \mid 28$ , etc.

**Reflexivity:** For every  $a \in \mathbb{Z} \setminus \{0\}$ , we have  $a \mid a$  and  $a \mid -a$ .

**Units:** For every  $a \in \mathbb{Z} \setminus \{0\}$ , we have  $1 \mid a$  and  $-1 \mid a$ .

**Zero Divisors:** If  $ab = 0$  then either  $a = 0$  or  $b = 0$ .

**Transitivity:** If  $a, b, c \in \mathbb{Z} \setminus \{0\}$  satisfy  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .

To see this, note that  $a \mid b$  and  $b \mid c$  means that there must be integers  $m, n \in \mathbb{Z}$  such that  $b = am$  and  $c = bn$ ; so that  $c = (am)n = a(mn)$ . Clearly  $mn \in \mathbb{Z}$ .

## Division of Integers

A slightly more complicated property is:

**Integer Linear Combination:** If  $a, b, c \in \mathbb{Z}$  satisfy  $a \mid b$  and  $a \mid c$ , then for every  $x, y \in \mathbb{Z}$  we have  $a \mid (bx + cy)$ .

To see this, note that  $a \mid b$  and  $a \mid c$  means that there are integers  $m, n \in \mathbb{Z}$  such that  $b = am$  and  $c = an$ .

Now  $bx + cy = (am)x + (an)y = a(mx + ny)$  and  $mn \in \mathbb{Z}$ .

A useful consequence of this is the **Rule of “2 out of 3”**:

Suppose  $x, y, z \in \mathbb{Z}$  are such that  $x + y = z$ , and there is  $a \in \mathbb{N}$  which divides two of  $x, y, z$ ; then  $a$  divides all three of  $x, y, z$ .

*Proof.* Since  $z = x + y = 1 \times x + 1 \times y$ ,

then  $x = z - y = 1 \times z + (-1) \times y$

and  $y = z - x = 1 \times z + (-1) \times x$ .

So whichever are the two known multiples of  $a$ , then the third can be written as an integer linear combination of these.

Hence the third is also a multiple of  $a$ . □